UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

PHARAH NOZIL, individually and on behalf of all others similarly situated, Plaintiff, v. WEIGHTLESS MEDICAL LLC, Defendant.	**Case No.** **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Pharah Nozil ("Plaintiff"), individually and on behalf of all others similarly situated, by and through her attorneys, makes the following allegations pursuant to the investigation of her counsel and based upon information and belief, except as to allegations specifically pertaining to herself, which are based on personal knowledge.

NATURE OF ACTION

1. This is a class action lawsuit brought on behalf of all persons who have visited the website joinweightcare.com (the "Website") and purchased prescription Glucagon-like peptide-1 ("GLP-1") weight loss medication.

2. Weightless Medical LLC ("Defendant") is an online provider of prescription GLP-1 weight loss medication.

3. When consumers visit the Website, they are first directed to, "Select Your Weight Loss Program," whereby they purchase subscription weight loss medication. Then, they "Connect With A WeightCare Doctor Online."[1]

[1] https://joinweightcare.com/pages/how-it-works

4. Unbeknownst to Plaintiff and members of the putative class, as they were making their purchases in real-time, Defendant disclosed their personally identifiable information and protected health information to third parties such as Meta Platforms, Inc. ("Meta") for targeted advertising purposes.

5. Plaintiff therefore brings this action for legal and equitable remedies resulting from Defendant's illegal actions.

THE PARTIES

6. At all relevant times Plaintiff Pharah Nozil was a resident of Brooklyn, New York. In approximately January 2024, Plaintiff purchased prescription GLP-1 medication through Defendant's Website. Unbeknownst to Plaintiff, Defendant disclosed her personal information—i.e. the details of her purchase of prescription weight loss medication—to third parties, including but not limited to Meta, for targeted advertising purposes. After purchasing her prescription weight loss medication on Defendant's Website, Plaintiff began receiving targeted advertisements for similar products and services. Plaintiff would not have booked an appointment on Defendant's Website if she knew Defendant was violating her privacy by sharing her personal information with unknown third parties.

7. Weightless Medical LLC is a Delaware corporation with its principal place of business in Delaware. Defendant develops, owns, and operates the Website, which is used by consumers throughout New York and the United States to book appointments for and purchase prescription weight loss medication.

JURISDICTION AND VENUE

8. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A) as modified by the Class Action Fairness Act of 2005, because at least one member of the Class,

as defined below, is a citizen of a different state than Defendant, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interests and costs.

9. This Court has personal jurisdiction over Defendant because Defendant conducts substantial business within this District.

10. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because a substantial part of the events giving rise to this claim occurred in this District.

FACTUAL ALLEGATIONS COMMON TO ALL CLAIMS

A. Health-Related Information is Sensitive and Confidential

11. Defendant assisted Meta with intercepting information that is sensitive, confidential, and personally identifiable.

12. Defendant is an online provider of GLP-1 weight loss medication.

13. Under federal law, a healthcare provider may not disclose personally identifiable information ("PII") or protected health information ("PHI") without the patient's express written authorization.[2] In this case, PHI includes but is not limited to information pertaining to medical prescriptions relating to GLP-1 weight loss medication.

14. The United States Department of Health and Human Services ("HHS") has established a national standard, known as the HIPAA Privacy Rule, to explain the duties healthcare providers owe to their patients. "The Rule requires appropriate safeguards to protect the privacy of [PHI] and sets limits and conditions on the uses and disclosures that may be made of such information without an individual's authorization."[3]

[2] HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502, 165.508(a), 164.514(b)(2)(i).

[3] U.S. Dept. of Health and Human Services, https://www.hhs.gov/hipaa/for-professionals/privacy/index.html.

15. A healthcare provider violates the HIPAA Privacy Rule if it knowingly and in violation of 42 U.S.C. §§ 1320d-d9 ("Part C"): "(1) uses of causes to be used a unique health identifier; [or] (2) obtains individually identifiable health information relating to an individual."[4]

16. The statute states that an entity "shall be considered to have obtained or disclosed individually identifiable health information in violation of [Part C] if the information is maintained by a covered entity…and the individual obtained or disclosed such information without authorization." *Id*.

17. The criminal and civil penalties imposed by 42 U.S.C. § 1320d-6 apply directly to Defendant when it is knowingly disclosing individually identifiable health information relating to its patients.

18. Defendant further failed to comply with other HIPAA safeguard regulations as follows:

a. Failing to ensure the confidentiality and integrity of electronic PHI that Defendant created, received, maintained and transmitted in violation of 45 C.F.R. Section 164.306(a)(1);

b. Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.R.F. Section 164.308(a)(1);

c. Failing to identify and respond to suspected or known security incidents and mitigate harmful effects of security incidents known to Defendant in violation of 45 C.F.R. Section 164.308(a)(6)(ii);

d. Failing to protect against reasonably anticipated threats or hazards to the

[4] 42 U.S.C. § 1320d-6.

security or integrity of electronic PHI in violation of 45 C.F.R. Section 306(a)(2);

e. Failing to protect against reasonably anticipated uses of disclosures of electronic PHI not permitted under privacy rules pertaining to individually identifiable health information in violation of 45 C.F.R. Section 164.306(a)(3); and

f. Failing to design, implement and enforce policies and procedures that would establish physical and administrative safeguards to reasonably safeguard PHI in violation of 45 C.F.R. Section 164.530(c).

19. Health care entities regulated under HIPAA, like Defendant, may use third-party tracking tools in a limited way to perform analysis on data key to operations. They are not permitted, however, to use these tools in a way that may expose patients' PHI to vendors (as shown below in Figures 3 through 7). As explained by a statement published by the HHS:

> Regulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules. **For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures**.[5]

20. The Bulletin discusses the types of harm that disclosure may cause to the patient:

> An impermissible disclosure of an individual's PHI not only violates the Privacy Rule but also may result in a wide range of additional harms to the individual or others. For example, an impermissible disclosure of PHI may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual's PHI. Such disclosures can reveal incredibly sensitive information about an individual, including diagnoses,

[5] HHS.gov, USE OF ONLINE TRACKING TECHNOLOGIES BY HIPAA COVERED ENTITIES AND BUSINESS ASSOCIATES (THE "BULLETIN") (EMPHASIS ADDED), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

> frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment. While it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors, **because of the proliferation of tracking technologies collecting sensitive information, now more than ever, it is critical for regulated entities to ensure that they disclose PHI only as expressly permitted or required by the HIPAA Privacy Rule.**[6]

21. Plaintiff and Class Members face exactly the risks about which the government expresses concern. Defendant's unlawful conduct resulted in third parties, including but not limited to Meta, intercepting information regarding Plaintiff and Class Members scheduling consultations on the Website.

22. The Bulletin goes on to make clear how broad the government's view of protected information is. It explains:

> This information might include an individual's medical record number, home or email address, or dates of appointments, as well as an individual's IP address or geographic location, medical device IDs, **or any unique identifying code**.[7]

23. Crucially, that paragraph in the government's Bulletin continues:

> All such [individually identifiable health information ("IIHI")] collected on a regulated entity's website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the IIHI, such as IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services. This is because, when a regulated entity collects the individual's IIHI through its website or mobile app, the information connects the individual to the regulated entity (i.e., it is indicative that the individual has received or will receive health care services or benefits from the covered entity), and thus relates to the individual's past, present, or future health or health care or payment for care.[8]

[6] *Id.* (emphasis added).

[7] *Id.* (emphasis added).

[8] *Id.*

24. Then, in July 2022, the Federal Trade Commission ("FTC") and the Department of Health and Human Services ("HHS") issued a joint press release warning regulated entities about the privacy and security risks arising from the use of online tracking technologies:

> The Federal Trade Commission and the U.S. Department of Health and Human Services' Office for Civil Rights (OCR) are cautioning hospitals and telehealth providers [regulated entities] about the privacy and security risks related to the use of online tracking technologies integrated into their websites or mobile apps that may be impermissibly disclosing consumers' sensitive personal health data to third parties.
>
> "When consumers visit a hospital's [regulated entity's] website or seek telehealth services, they should not have to worry that their most private and sensitive health information may be disclosed to advertisers and other unnamed, hidden third parties," said Samuel Levine, Director of the FTC's Bureau of Consumer Protection. "The FTC is again serving notice that companies need to exercise extreme caution when using online tracking technologies and that we will continue doing everything in our powers to protect consumers' health information from potential misuse and exploitation."
>
> "Although online tracking technologies can be used for beneficial purposes, patients and others should not have to sacrifice the privacy of their health information when using a hospital's [regulated entity's] website," said Melanie Fontes Rainer, OCR Director. "OCR continues to be concerned about impermissible disclosures of health information to third parties and will use all of its resources to address this issue."
>
> The two agencies sent the joint letter to approximately 130 [regulated entities] hospital systems and telehealth providers to alert them about the risks and concerns about the use of technologies, such as the Meta/Facebook pixel and Google Analytics, that can track a user's online activities. These tracking technologies gather identifiable information about users, usually without their knowledge and in ways that are hard for users to avoid, as users interact with a website or mobile app.
>
> In their letter, both agencies reiterated the risks posed by the unauthorized disclosure of an individual's personal health information to third parties. For example, the disclosure of such information could reveal sensitive information including health conditions, diagnoses, medications, medical treatments, frequency of visits to health care professionals, and where an individual seeks medical treatment.[9]

[9] Federal Trade Commission, *FTC and HHS Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies*, July 20, 2023,

25. Therefore, Defendant's conduct, as described more thoroughly below, is directly contrary to federal law and the clear pronouncements by the FTC and HHS.

B. The Facebook Tracking Pixel

26. Facebook, owned by Meta, describes itself as a "real identity platform,"10 meaning users are allowed only one account and must share "the name they go by in everyday life."[11] To that end, when creating an account, users must provide their first and last name, along with their birthday and gender.[12]

27. Meta sells advertising space by highlighting its ability to target users.[13] Meta can target users so effectively because it surveils user activity both on and off its sites.[14] This allows Meta to make inferences about users beyond what they explicitly disclose, like their "interests," "behavior," and "connections."[15] Meta compiles this information into a generalized dataset called "Core Audiences," which allows advertisers to reach precise audiences based on specified targeting types.[16]

---

https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking.

[10] Sam Schechner and Jeff Horwitz, *How Many Users Does Facebook Have? The Company Struggles to Figure It Out*, WALL. ST. J. (Oct. 21, 2021).

[11] FACEBOOK, COMMUNITY STANDARDS, PART IV INTEGRITY AND AUTHENTICITY, https://www.facebook.com/communitystandards/integrity_authenticity.

[12] FACEBOOK, SIGN UP, https://www.facebook.com.

[13] FACEBOOK, WHY ADVERTISE ON FACEBOOK, INSTAGRAM AND OTHER META TECHNOLOGIES, https://www.facebook.com/business/help/205029060038706.

[14] FACEBOOK, ABOUT META PIXEL, https://www.facebook.com/business/help/742478679120153?id=1205376682832142.

[15] FACEBOOK, AD TARGETING: HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, https://www.facebook.com/business/ads/ad-targeting.

[16] https://www.facebook.com/business/news/Core-Audiences.

28. Advertisers can also build "Custom Audiences."[17] Custom Audiences enables advertisers to reach "people who have already shown interest in [their] business, whether they're loyal customers or people who have used [their] app or visited [their] website."[18] With Custom Audiences, advertisers can target existing customers directly, and they can also build "Lookalike Audiences," which "leverage[] information such as demographics, interests, and behavior from your source audience to find new people who share similar qualities."[19] Unlike Core Audiences, advertisers can build Custom Audiences and Lookalike Audiences only if they first supply Meta with the underlying data. They can do so through two mechanisms: by manually uploading contact information for customers or by utilizing Meta's "Business Tools."[20]

29. As Meta puts it, the Business Tools "help website owners and publishers, app developers, and business partners, including advertisers and others, integrate with [Facebook], understand and measure their products and services, and better reach and serve people who might be interested in their products and services."[21] Put more succinctly, Meta's Business Tools are bits of code that advertisers can integrate into their websites, mobile applications, and servers, thereby enabling Meta to intercept and collect user activity on those platforms.

---

[17] FACEBOOK, ABOUT CUSTOM AUDIENCES, https://www.facebook.com/business/help/744354708981227?id=2469097953376494.

[18] FACEBOOK, AD TARGETING, HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, https://www.facebook.com/business/ads/ad-targeting.

[19] FACEBOOK, ABOUT LOOKALIKE AUDIENCES, https://www.facebook.com/business/help/164749007013531?id=401668390442328.

[20] FACEBOOK, CREATE A CUSTOMER LIST CUSTOM AUDIENCE, https://www.facebook.com/business/help/170456843145568?id=2469097953376494; FACEBOOK, CREATE A WEBSITE CUSTOM AUDIENCE, https://www.facebook.com/business/help/1474662202748341?id=2469097953376494.

[21] FACEBOOK, THE META BUSINESS TOOLS, https://www.facebook.com/help/331509497253087.

30. The Business Tools are automatically configured to capture certain data, like when a user visits a webpage, that webpage's Universal Resource Locator ("URL") and metadata, or when a user downloads a mobile application or makes a purchase.[22] Meta's Business Tools can also track other events. Meta offers a menu of "standard events" from which advertisers can choose, including what content a visitor views or purchases.[23] Advertisers can even create their own tracking parameters by building a "custom event."[24]

31. One such Business Tool is the Facebook Pixel (the "Facebook Pixel"). Meta offers this piece of code to advertisers, like Defendant, to integrate into their websites. The Facebook Pixel "tracks the people and type of actions they take."[25] When a user accesses a website hosting the Facebook Pixel, Meta's software script surreptitiously directs the user's browser to contemporaneously send a separate message to Meta's servers. This secret and contemporaneous transmission contains the original GET request sent to the host website, along with additional data that the Facebook Pixel is configured to collect. This transmission is initiated by Meta code and concurrent with the communications with the host website. At

---

[22] *See* FACEBOOK, META FOR DEVELOPERS: META PIXEL, ADVANCED, https://developers.facebook.com/docs/meta-pixel/advanced/; *see also* FACEBOOK, BEST PRACTICES FOR META PIXEL SETUP, https://www.facebook.com/business/help/218844828315224?id=1205376682832142; FACEBOOK, META FOR DEVELOPERS: MARKETING API - APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/.

[23] FACEBOOK, SPECIFICATIONS FOR META PIXEL STANDARD EVENTS, https://www.facebook.com/business/help/402791146561655?id=1205376682832142.

[24] FACEBOOK, ABOUT STANDARD AND CUSTOM WEBSITE EVENTS, https://www.facebook.com/business/help/964258670337005?id=1205376682832142; *see also* FACEBOOK, META FOR DEVELOPERS: MARKETING API – APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/.

[25] FACEBOOK, RETARGETING, https://www.facebook.com/business/goals/retargeting.

relevant times, two sets of code were thus automatically run as part of the browser's attempt to load and read Defendant's Website—Defendant's own code and Facebook's embedded code.

32. Each time Defendant sent this activity data, it also disclosed a patient's personally identifiable information, including their Facebook ID ("FID"). An FID is a unique and persistent identifier that Facebook assigns to each user. With it, any ordinary person can look up the user's Facebook profile and name. Notably, while Meta can easily identify any individual on its Facebook platform with only their unique FID, so too can any ordinary person who comes into possession of an FID. Meta admits as much on its website. Indeed, ordinary persons who come into possession of the FID can connect to any Facebook profile.

33. A user who accessed Defendant's Website while logged into Facebook transmitted what is known as a "c_user cookie" to Facebook, which contained that user's unencrypted Facebook ID.

34. The Facebook Pixel is designed to collect information about website visitors that can be matched to an individual's Facebook profile for the purpose of sending targeted advertising to that user.

35. When the Facebook Pixel is used on a website, it is not like a tape recorder or a "tool" used by one party to record the other. Instead, the Facebook Pixel involves Meta, a separate and distinct third-party entity from the parties in the conversation, using the Facebook Pixel to eavesdrop on, record, extract information from, and analyze a conversation to which it is not a party. This is so because Meta itself is collecting the content of any conversation. That information is then analyzed by Meta before being provided to any entity that was a party to the conversation (like Defendant).

36. Once Meta intercepts website communications, it has the capability to use such information for its own purposes. In 2021, Meta generated over $117 billion in revenue.[26] With respect to the apps offered by Meta, substantially all of Meta's revenue is generated by selling advertising space.[27] Meta sells advertising space by highlighting its ability to target users by including them in the Core Audiences and Custom Audiences offered to its clients.[28]

37. In practice, this means the information collected is used to (i) analyze trends in consumer behavior based on data collected from websites across the internet that Meta can then use when providing targeted advertising to other companies, (ii) create consumer profiles of specific users, allowing Meta to sell future customers targeted advertising to consumers with specific profile characteristics, and (iii) develop new Meta Business Tools products and services, or improve pre-existing Meta Business Tools products and services.

38. One of Meta's partners is Defendant. The Facebook Pixel is employed on the Website in the manner described throughout this Complaint.

C. Defendant Violates the Privacy Rights of its Customers

39. GLP-1 medications, such as Ozempic, are surging in popularity. These medications are expected to reach $150 billion in sales within the next ten years.[29]

---

[26] FACEBOOK, META ANNUAL REPORT 2021, https://s21.q4cdn.com/399680738/files/doc_financials/annual_reports/2023/2021-Annual-Report.pdf at 51.

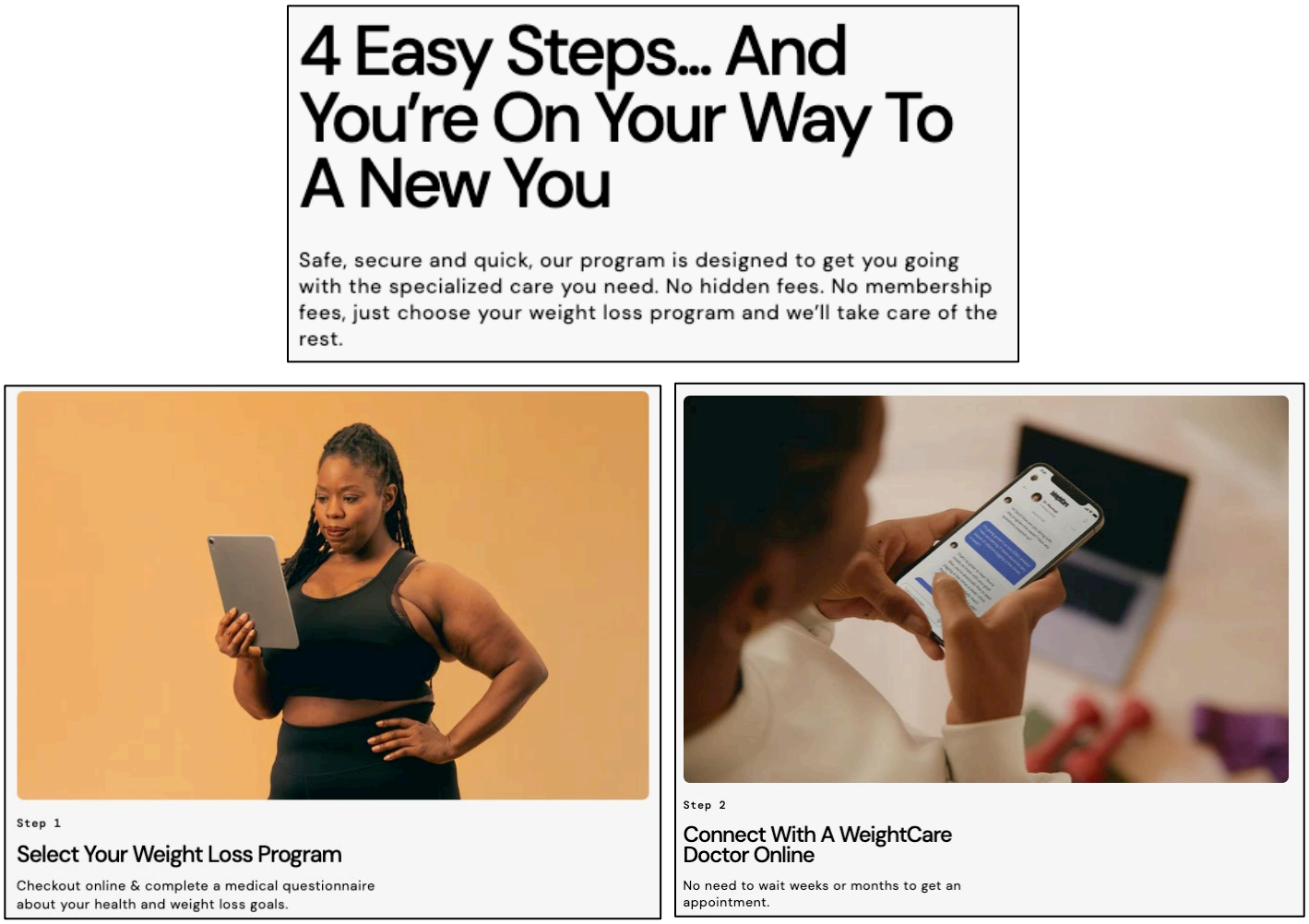
[27] *Id.* at 63.

[28] FACEBOOK, WHY ADVERTISE ON FACEBOOK, INSTAGRAM AND OTHER META TECHNOLOGIES, https://www.facebook.com/business/help/205029060038706.

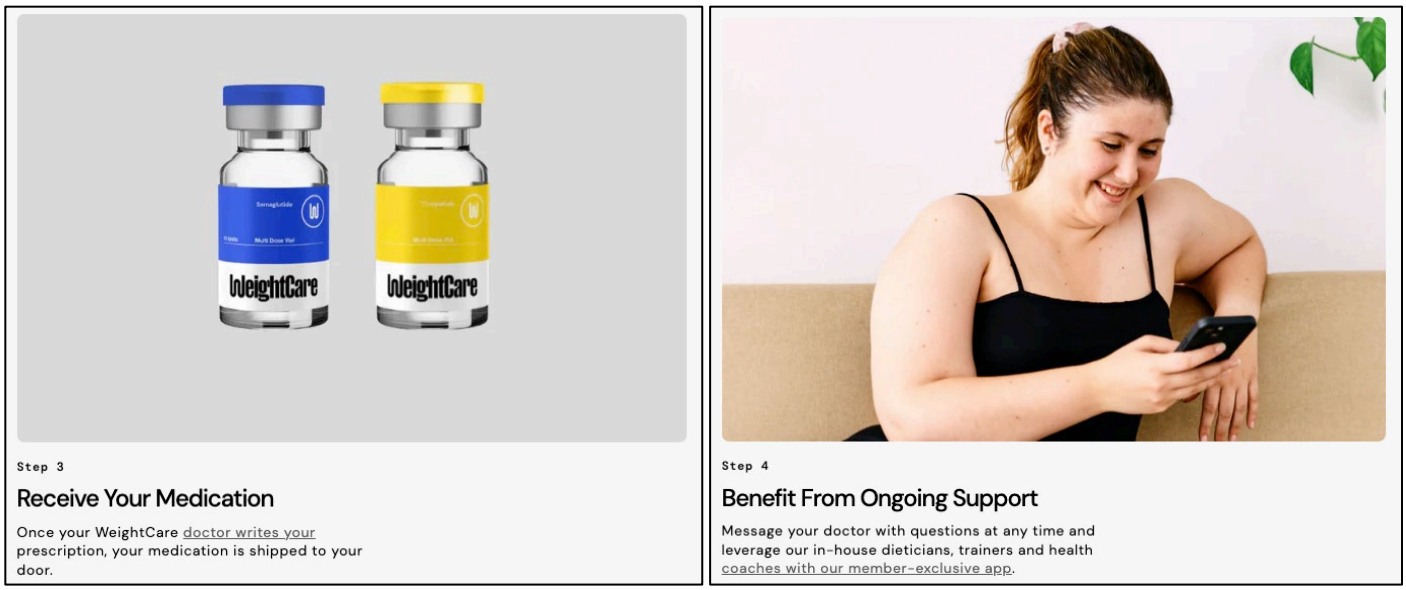
[29] Beasley, Deena, *Weight-loss drug forecasts jump to $150 billion as supply grows*, Reuters (May 28, 2024).

40. Defendant requires prospective customers to purchase the weight loss medication prior to "connect[ing] with a WeightCare doctor" to determine whether they qualify for weight loss medication. Defendant requests personal information from consumers, such as their name, email address, and phone number. Defendant also requests information relating to height and weight, and whether the prospective customer is pregnant, breastfeeding, or planning to become pregnant. Unbeknownst to consumers, and contrary to Defendant's representation that its medication purchase process is "secure,"[30] Defendant shares this information—along with the specific weight loss medication purchased—with third parties for targeted advertising purposes.

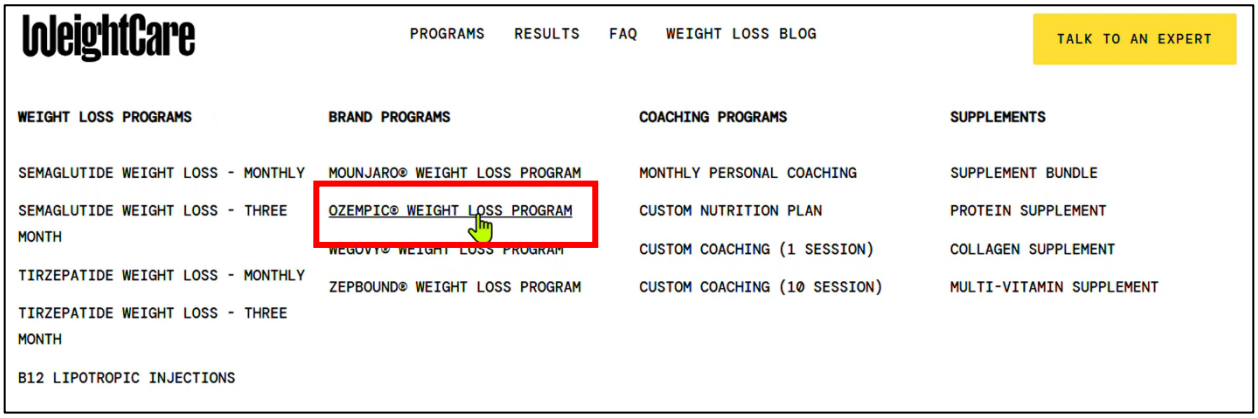
41. Defendant describes the medication purchase process in "4 Easy Steps…":



[30] https://joinweightcare.com/pages/how-it-works



42. Patients begin Step 1 by selecting a prescription weight loss medication to purchase:



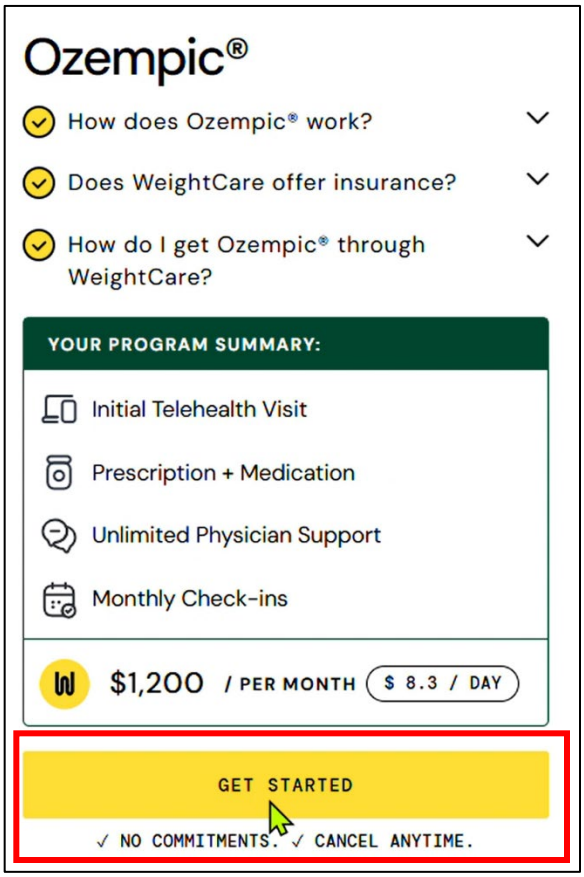
43. However, unbeknownst to its patients, Defendant discloses this confidential information to its advertising partner, Meta, as demonstrated below:

Facebook - Product Page View
https://www.facebook.com/tr/?
Fri Jan 31 16:39:20 EST 2025

Cookies:
datr qWJPZ_e1vlFpWf108Hg0viQ-
sb qWJPZ3EtTh2IMGUDnurGmNgr
c_user 61557047663647
xs 34%3AHRvYMa6M9M6FUQ%3A2%3A1733255868%3A-1%3A-1
fr 0mPHdxWuN2bS6AYHJ.AWWE364nA1j8YFfP5pgrecQlccw.BnT2Kp..AAA.0.0.BnT2K-.AWX9fZxcS5g
ar_debug 1

Data:
id 6265563013468142
ev ViewContent
dl https%3A%2F%2Fjoinweightcare.com%2Fproducts%2Fozempic
rl https%3A%2F%2Fjoinweightcare.com%2F
if false
ts 1738359560284
cd[content_ids] %5B9644388483376%5D
cd[content_type] product_group
cd[content_name] Ozempic%C2%AE
cd[content_category] branded
cd[currency] USD
cd[value] 1200
sw 3072

44. After confirming their selection and continuing to purchase their prescription medications, Defendant discloses that information to Meta through the Facebook Tracking Pixel as well:



Facebook - Initiate Checkout
https://www.facebook.com/tr/?
Fri Jan 31 16:39:27 EST 2025

Cookies:
datr qWJPZ_e1vlFpWf108Hg0viQ-
sb qWJPZ3EtTh2IMGUDnurGmNgr
c_user 61557047663647
xs 34%3AHRvYMa6M9M6FUQ%3A2%3A1733255868%3A-1%3A-1
fr 0mPHdxWuN2bS6AYHJ.AWWE364nA1j8YFfP5pgrecQlccw.BnT2Kp..AAA.0.0.BnT2K-.AWX9fZxcS5g
ar_debug 1

Data:
id 6265563013468142
ev InitiateCheckout
dl https%3A%2F%2Fjoinweightcare.com%2Fcheckouts%2Fcn%2FZ2NwLXVzLWVhc3QxOjAxSkpaNFZDUzgwQ1ZWS1hQNUM4RUhWM01K
rl https%3A%2F%2Fjoinweightcare.com%2Fproducts%2Fozempic
if false
ts 1738359567387
cd[content_ids] %5B9644388483376%5D
cd[content_type] product_group
cd[currency] USD
cd[value] 1200
cd[num_items] 1

45. As shown above, Plaintiff's communications with Defendant were disclosed by Defendant to Meta and/or intercepted in transit by Meta, in real time, via detailed URLs, which contain the medically sensitive information and personally identifiable information entered into the Website. Such findings were also confirmed by Plaintiff's offsite activity report from her personal Facebook account.

46. Defendant further assists Meta by disclosing the PII of its patients sufficient for Meta to uncover their identities, as each transmission is accompanied by the patient's Facebook ID.

47. As shown above, Plaintiff's communications with Defendant were disclosed by Defendant to Meta and/or intercepted in transit by Meta, in real time, via detailed URLs, which contain medically sensitive information and personally identifiable information entered into the Website.

48. When patients share their personal information with medical professionals, they expect this information to be kept confidential. Moreover, when consumers seek a medical consultation with a physician and/or purchase prescription medication from medical professionals, they also expect this highly sensitive information to be kept confidential.

49. If patients knew that Defendant was sharing their personal information for targeted advertising purposes, they would go to one of its competitors who do not engage in surreptitious data collection and disclosure to unknown third parties.

50. Through Meta's tracking services, which Defendant used via the software code installed, integrated and embedded into the Website, Defendant disclosed its patients' identities and sensitive medical information.

51. By installing, integrating and embedding the above-listed tracking technologies into the Website, and by directing such installation, integration and embedding, Defendant aided and conspired with third parties, including but not limited to Meta, and others to allow those third-party entities to contemporaneously and surreptitiously intercept the Website communications of Defendant's customers without customer consent.

52. Defendant engages in this deceptive conduct for its own profit at the expense of its patients. Such disclosures are an invasion of privacy, lead to harassing targeted advertising, and violates federal law.

CLASS ACTION ALLEGATIONS

53. Plaintiff brings this action on behalf of all persons in the United States who have a Facebook account and made a purchase on joinweightcare.com (the "Class").

54. Excluded from the Class is Defendant, the officers and directors of the Defendant at all relevant times, members of their immediate families and their legal representatives, heirs, successors or assigns and any entity in which either Defendant has or had a controlling interest.

55. Plaintiff is a member of the Class she seeks to represent.

56. The Class is so numerous that joinder of all members is impractical. Although Plaintiff does not yet know the exact size of the Class, Defendant claims to have "50,000+ Members."[31]

57. The Class is ascertainable because the Class members can be identified by objective criteria and through Defendant's own recordkeeping. Individual notice can be provided to Class members "who can be identified through reasonable effort." Fed. R. Civ. P. 23(c)(2)(B).

[31] https://joinweightcare.com/

58. There are numerous questions of law and fact common to the Class, which predominate over any individual actions or issues, including but not limited to:

A. Whether Defendant gave the Class members a reasonable expectation of privacy that their information was not being shared with third parties;

B. Whether Defendant's disclosure of information constitutes a violation of the claims asserted;

C. Whether Plaintiff and Class members are entitled to declaratory and/or injunctive relief to enjoin the unlawful conduct alleged herein; and

D. Whether Plaintiff and Class members have sustained damages as a result of Defendant's conduct and if so, what is the appropriate measure of damages or restitution.

59. Plaintiff's claims are typical of the claims of the members of the Class, as all members are similarly affected by Defendant's wrongful conduct. Plaintiff has no interests antagonistic to the interests of the other members of the Class. Plaintiff and all members of the Class have sustained economic injury arising out of Defendant's violations of common and statutory law as alleged herein.

60. Plaintiff is an adequate representative of the Class because her interests do not conflict with the interests of the Class members she seeks to represent, she has retained counsel competent and experienced in prosecuting class actions, and she intends to prosecute this action vigorously. The interests of Class members will be fairly and adequately protected by Plaintiff and her counsel.

61. The class mechanism is superior to other available means for the fair and efficient adjudication of the claims of Plaintiff and Class members. Each individual Class member may

lack the resources to undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Defendant's liability. Individualized litigation increases the delay and expense to all parties and multiplies the burden on the judicial system presented by the complex legal and factual issues of this case. Individualized litigation also presents a potential for inconsistent or contradictory judgments. In contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court on the issue of Defendant's liability. Class treatment of the liability issues will ensure that all claims are consistently adjudicated.

62. Plaintiff reserves the right to revise the foregoing class allegations and definitions based on facts learned and legal developments following additional investigation, discovery, or otherwise.

CAUSES OF ACTION

COUNT I
Violation of the Electronic Communications Privacy Act
18 U.S.C. § 2511(1), *et seq.*

63. Plaintiff incorporates by reference the allegations contained in the paragraphs above as if fully set forth herein.

64. Plaintiff brings this claim on behalf of herself and members of the nationwide Class.

65. The Electronic Communications Privacy Act ("ECPA") prohibits the intentional interception of the content of any electronic communication. 18 U.S.C. § 2511.

66. The ECPA protects both sending and the receipt of communications.

67. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

68. The transmission of Plaintiff's PII and PHI to Defendant's Website qualify as a "communication" under the ECPA's definition of 18 U.S.C. § 2510(12).

69. The transmission of PII and PHI between Plaintiff and Class Members and Defendant's Website with which they chose to exchange communications are "transfer[s] of signs, signals, writing,…data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(12).

70. The ECPA defines "contents," when used with respect to electronic communications, to "include[] any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. 18 U.S.C. § 2510(8).

71. The ECPA defines an interception as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

72. The ECPA defines "electronic, mechanical, or other device," as "any device…which can be used to intercept a[n]…electronic communication[.]" 18 U.S.C. § 2510(5).

73. The following instruments constitute "devices" within the meaning of the ECPA:

a. The computer codes and programs Defendant and third parties used to track Plaintiff and Class Members communications while they were

navigating the Website;

b. Plaintiff's and Class Members' browsers;

c. Plaintiff's and Class Members' mobile devices;

d. Defendant and Meta's web and ad servers;

e. The plan Defendant and the above-listed third parties carried out to effectuate the tracking and interception of Plaintiff's and Class Members' communications while they were using a web browser to navigate the Website.

74. Plaintiff and Class Members' interactions with Defendant's Website are electronic communications under the ECPA.

75. By utilizing and embedding the tracking technology provided by Meta on its Website, Defendant intentionally intercepted, endeavored to intercept, and/or procured another person to intercept, the electronic communications of Plaintiff and Class Members in violation of 18 U.S.C. § 2511(1)(a).

76. Specifically, Defendant intercepted—in real time—Plaintiff's and Class Members' electronic communications via the tracking technology provided by Meta on its Website, which tracked, stored and unlawfully disclosed Plaintiff's and Class Members' PII and PHI to third parties, including but not limited to Meta.

77. Defendant intercepted communications that include, but are not necessarily limited to, communications to/from Plaintiff and Class Members regarding PII and PHI, including their identities and weight loss medication prescription purchase information. This confidential information is then monetized for targeted advertising purposes, among other things.

78. By intentionally disclosing or endeavoring to disclose Plaintiff's and Class Members' electronic communications to affiliates and other third parties, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c).

79. By intentionally using, or endeavoring to use, the contents of Plaintiff's and Class Members' electronic communications, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

80. Defendant intentionally intercepted the contents of Plaintiff's and Class Members' electronic communications for the purpose of committing a criminal or tortious act in violation of the Constitution or laws of the United States or of any state, namely, invasion of privacy, among others.

81. The party exception in 18 U.S.C. § 2511(2)(d) does not permit a party that intercepts or causes interception to escape liability if the communication is intercepted for the purpose of committing any tortious or criminal act in violation of the Constitution or laws of the United States or of any State. Here, as alleged above, Defendant violated a provision of the Health Insurance Portability and Accountability Act, specifically 42 U.S.C. § 1320d-6(a)(3). This provision imposes a criminal penalty for knowingly disclosing individually identifiable health information ("IIHI") to a third party. HIPAA defines IIHI as:

> any information, including demographic information collected from an individual, that—(A) is created or received by a health care provider ... (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and (i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the

information can be used to identify the individual.[32]

82. Plaintiff's information that Defendant disclosed to Meta qualifies as IIHI, and Defendant violated Plaintiff's and Class Members' expectations of privacy. Such conduct constitutes tortious and/or criminal conduct through a violation of 42 U.S.C. § 1320d-6. Defendant used the electronic communications to increase its profit margins. Defendant specifically used the tracking technology provided by Meta to track and utilize Plaintiff's and Class Members' PII and PHI for financial gain.

83. Defendant was not acting under the color of law to intercept Plaintiff's and Class Members' wire or electronic communications.

84. Plaintiff and Class Members did not authorize Defendant to acquire the content of their communications for purposes of invading Plaintiff's and Class Members' privacy. Plaintiff and Class Members, all of whom are patients of Defendant, had a reasonable expectation that Defendant would not redirect their communications to Meta without their knowledge or consent.

85. The foregoing acts and omission therefore constitute numerous violations of 18 U.S.C. § 2511(1), *et seq*.

86. As a result of each and every violation thereof, on behalf of herself and the Class, Plaintiff seeks statutory damages of $10,000 or $100 per day for each violation of 18 U.S.C. § 2510, et seq. under 18 U.S.C. § 2520.

WHEREFORE, Plaintiff prays for relief and judgment, as follows:

a. Determining that this action is a proper class action;

[32] 42 U.S.C. § 1320d-6.

b. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure, naming Plaintiff as representative of the Class and naming Plaintiff's attorneys as Class Counsel to represent the Class;

c. For an order declaring that Defendant's conduct violates the statutes referenced herein;

d. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

e. Award compensatory damages, including statutory damages where available, to Plaintiff and the Class members against Defendant for all damages sustained as a result of Defendant's wrongdoing, in an amount to be proven at trial;

f. Ordering Defendant to disgorge revenues and profits wrongfully obtained;

g. For prejudgment interest on all amounts awarded;

h. For injunctive relief ordering Defendant to immediately cease its illegal conduct;

i. For an order awarding Plaintiff and the Class their reasonable attorneys' fees and expenses and costs of suit; and

j. Grant Plaintiff and the Class members such further relief as the Court deems appropriate.

JURY DEMAND

Plaintiff hereby demands a trial by jury on all claims so triable in this action.

Dated: March 5, 2025

Respectfully submitted,

By: */s/ Alec Leslie*

BURSOR & FISHER, P.A.
Alec M. Leslie
1330 Avenue of the Americas, 32nd Floor
New York, NY 10019

Tel: (646) 837-7150
Fax: (212) 989-9163
E-Mail: aleslie@bursor.com

BURSOR & FISHER, P.A.
Stephen A. Beck (*pro hac vice* forthcoming)
701 Brickell Ave., Suite 2100
Miami, FL 33131
Tel: (305) 330-5512
Fax: (305) 676-9006
E-Mail: sbeck@bursor.com

Attorneys for Plaintiff